BEST AVAILABLE COPY

10/500983
Rec'd PCT/PTO 06 JUL 2004

Figure 1

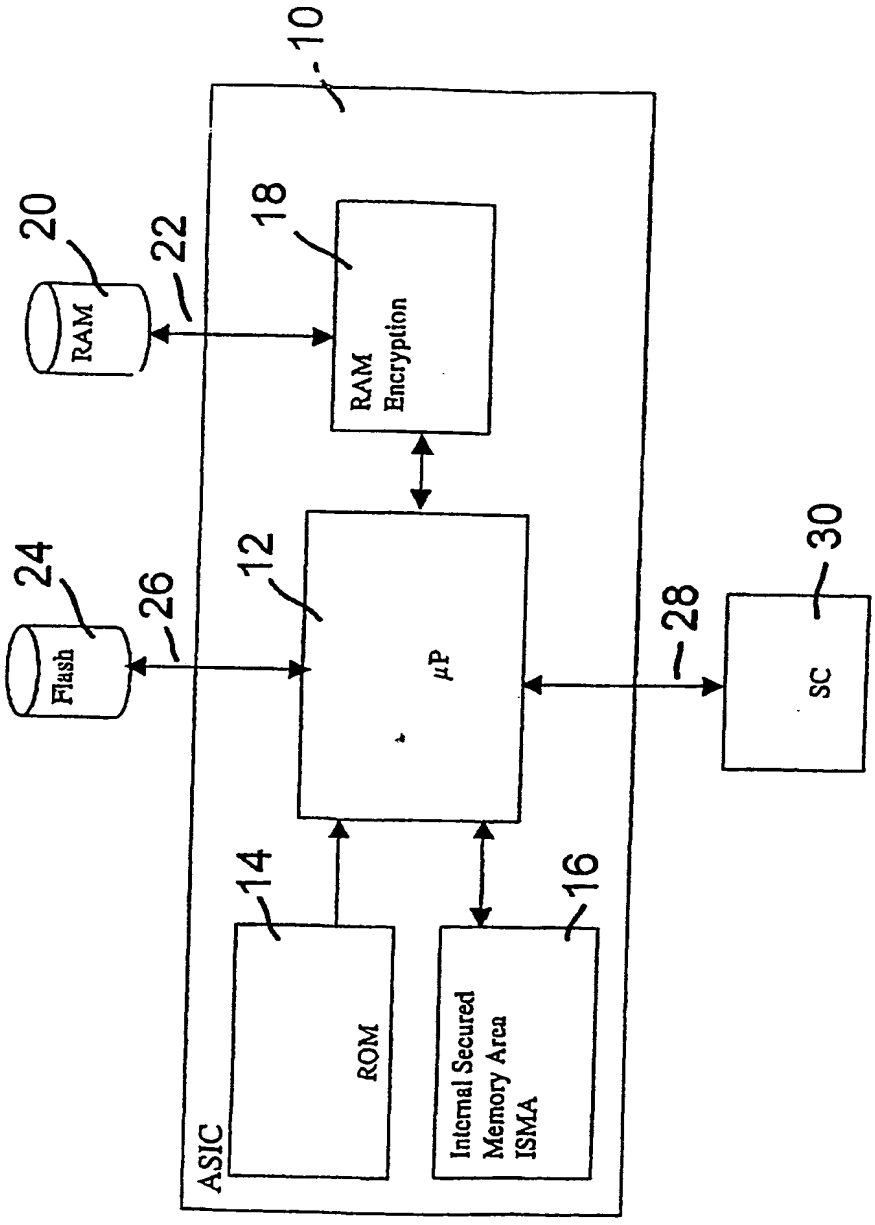
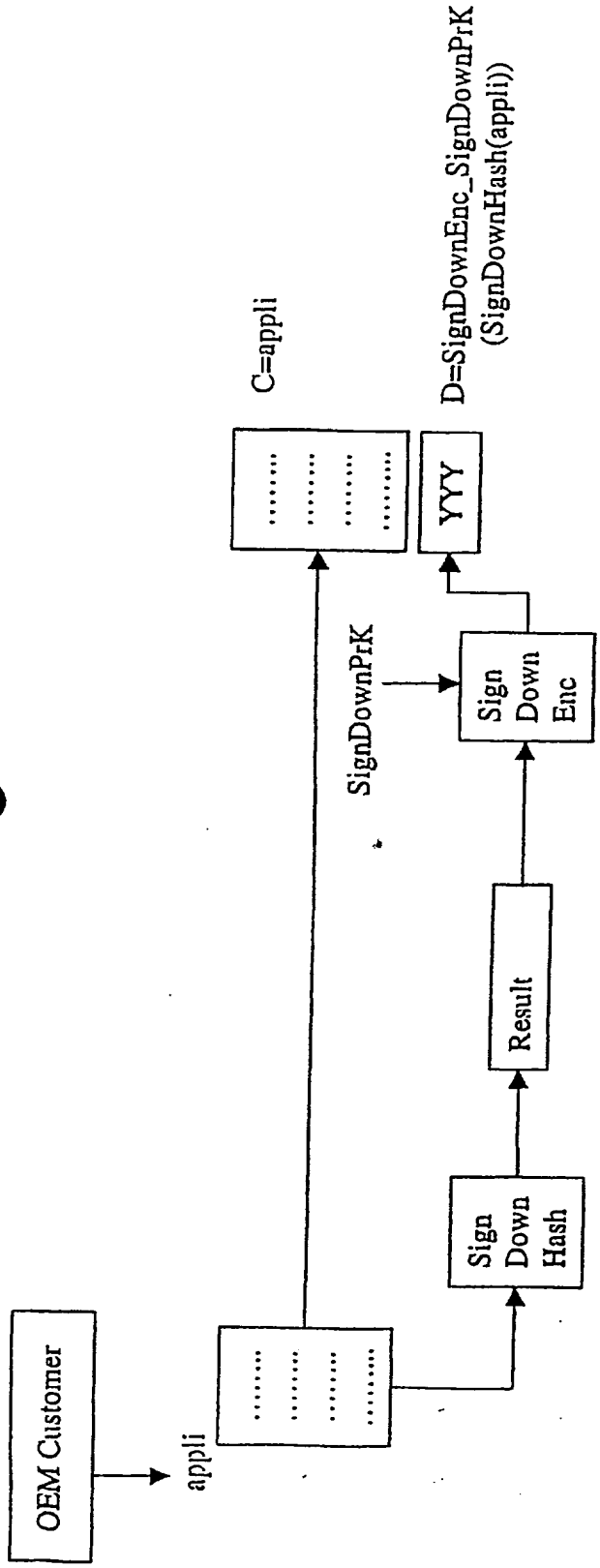
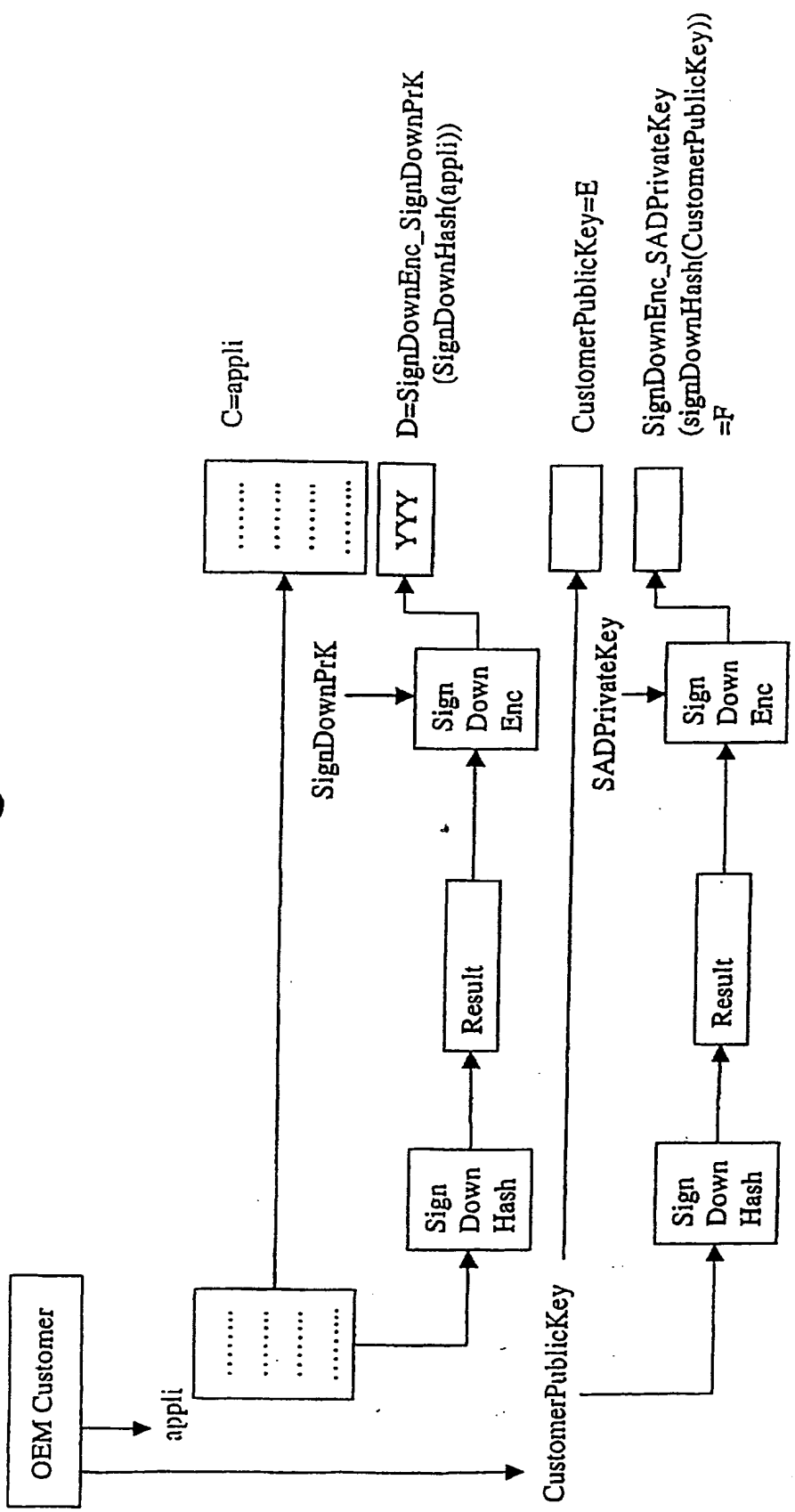


Figure 2A


OEM Customer
appli
Sign Down Hash
Result
SignDownPrK
Sign Down Enc
C=appli
D=SignDownEnc_SignDownPrK (SignDownHash(appli))
YYY

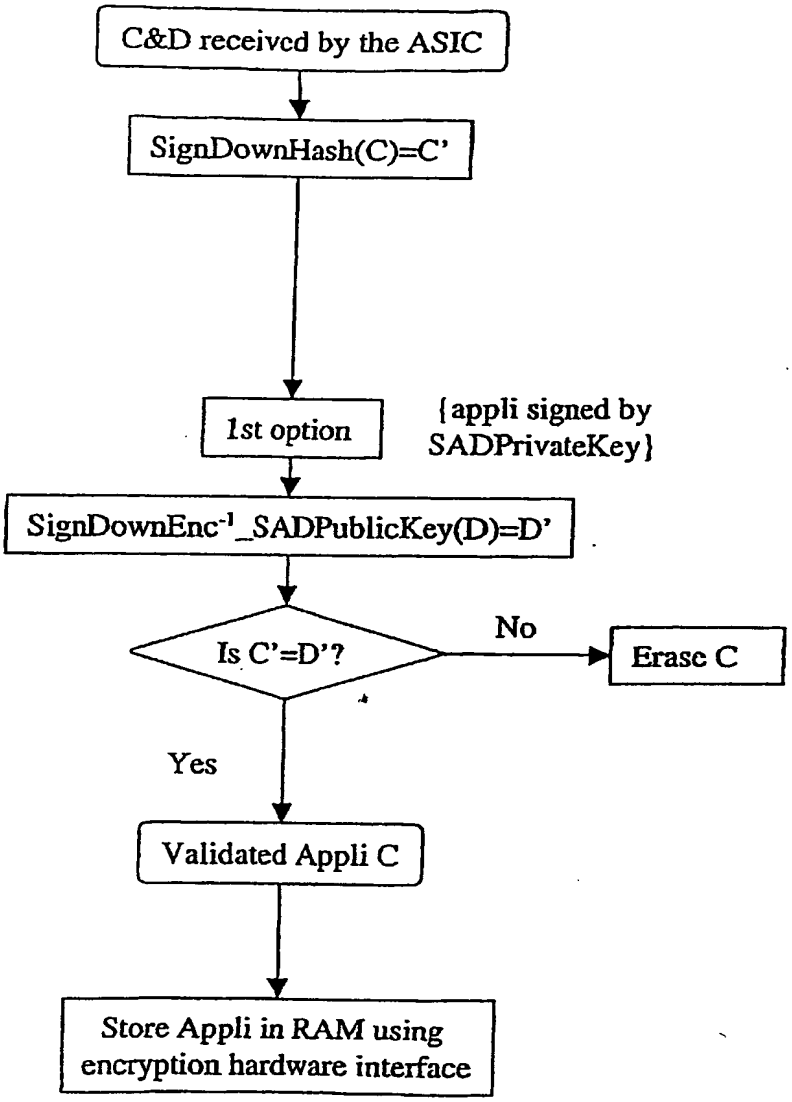
10/500983
Rec'd PCT/PTO 06 JUL 2004

Figure 2B



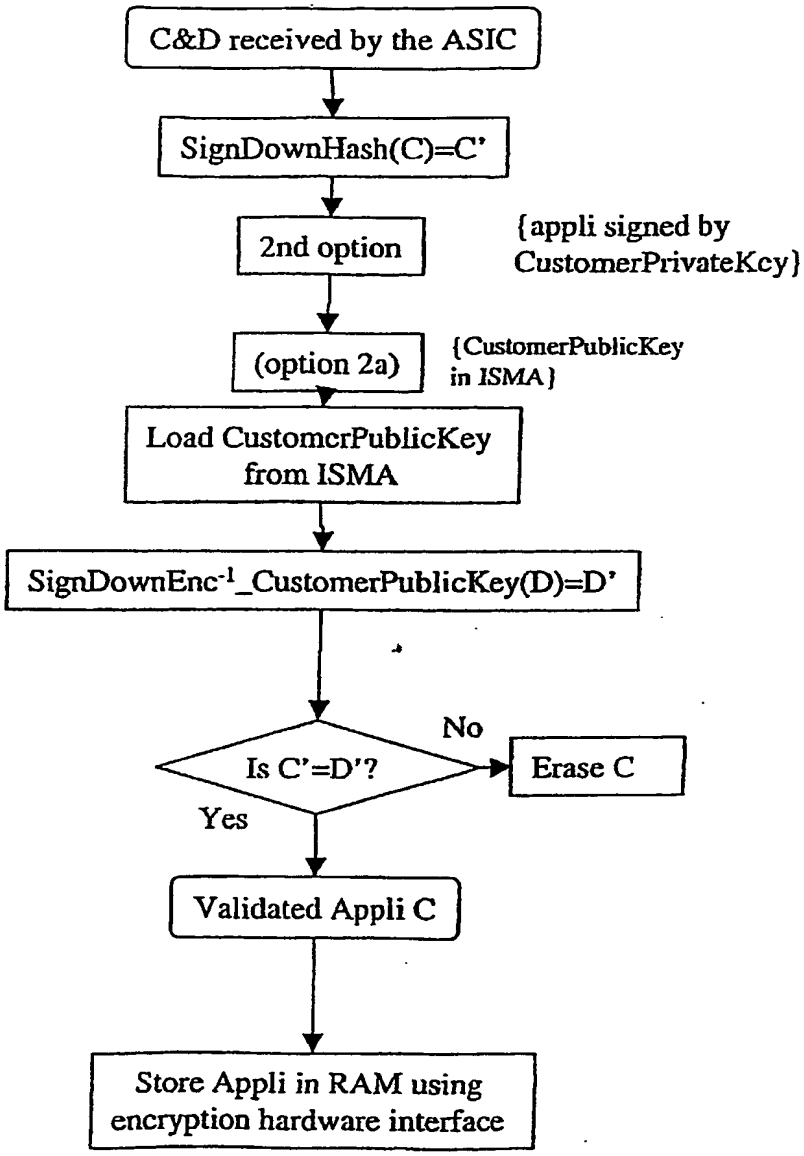
10/500983
Rec'd PCT/PTO 06 JUL 2004

figure 3A



10/500002
Rec'd PCT/PTO 06 JUL 2004

figure 3B



10/500983
Rec'd PCT/PTO 06 JUL 2004

Figure 3C

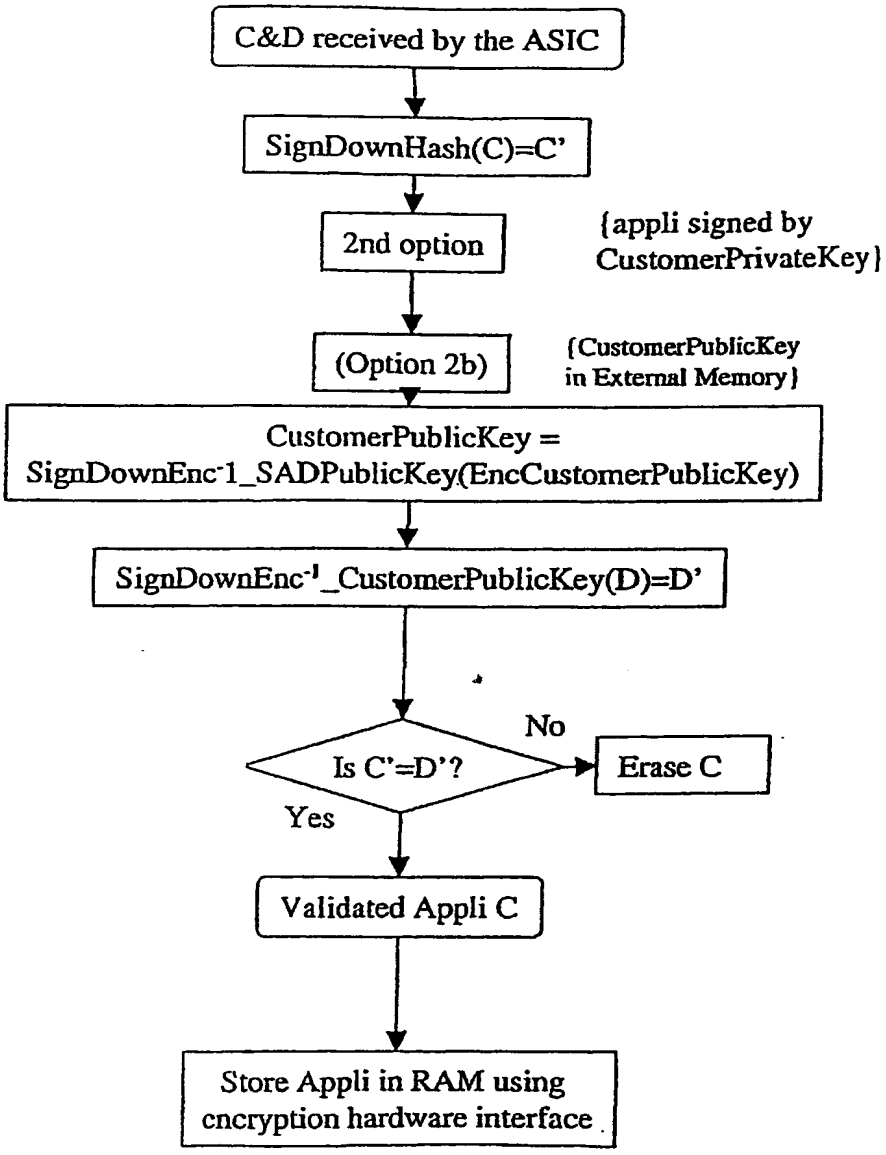
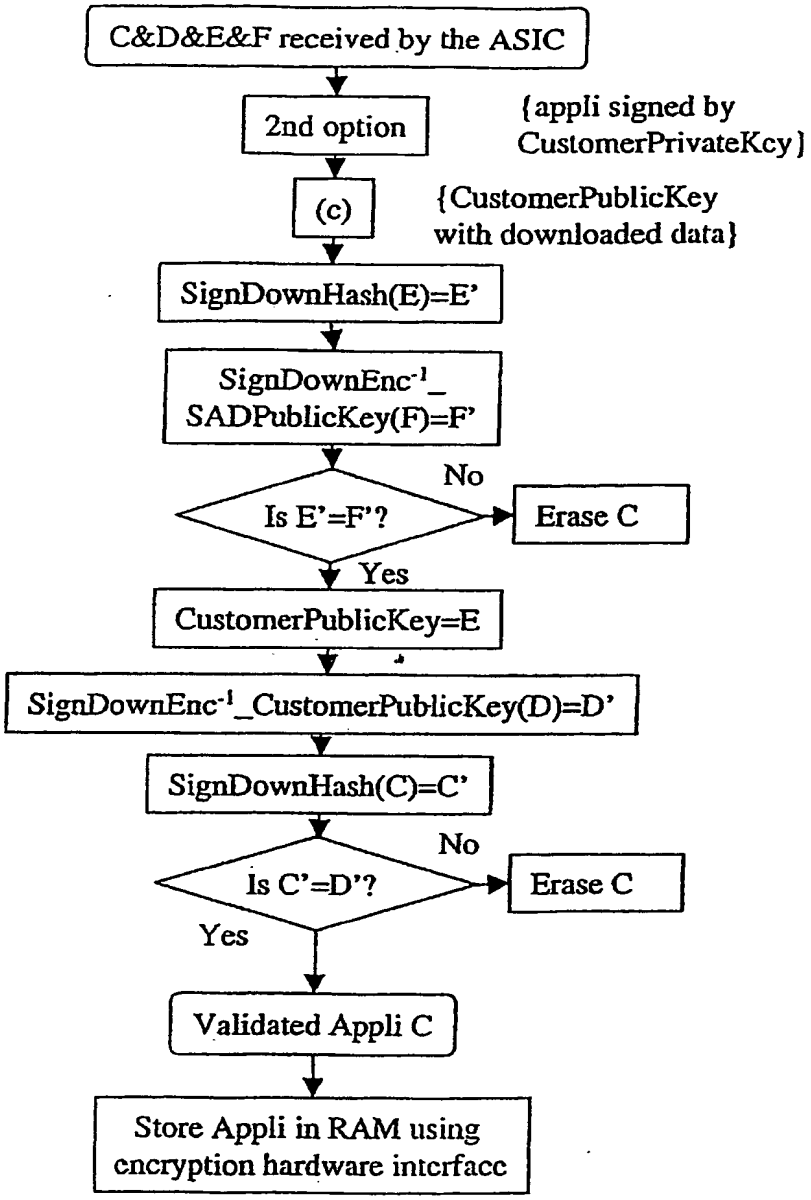
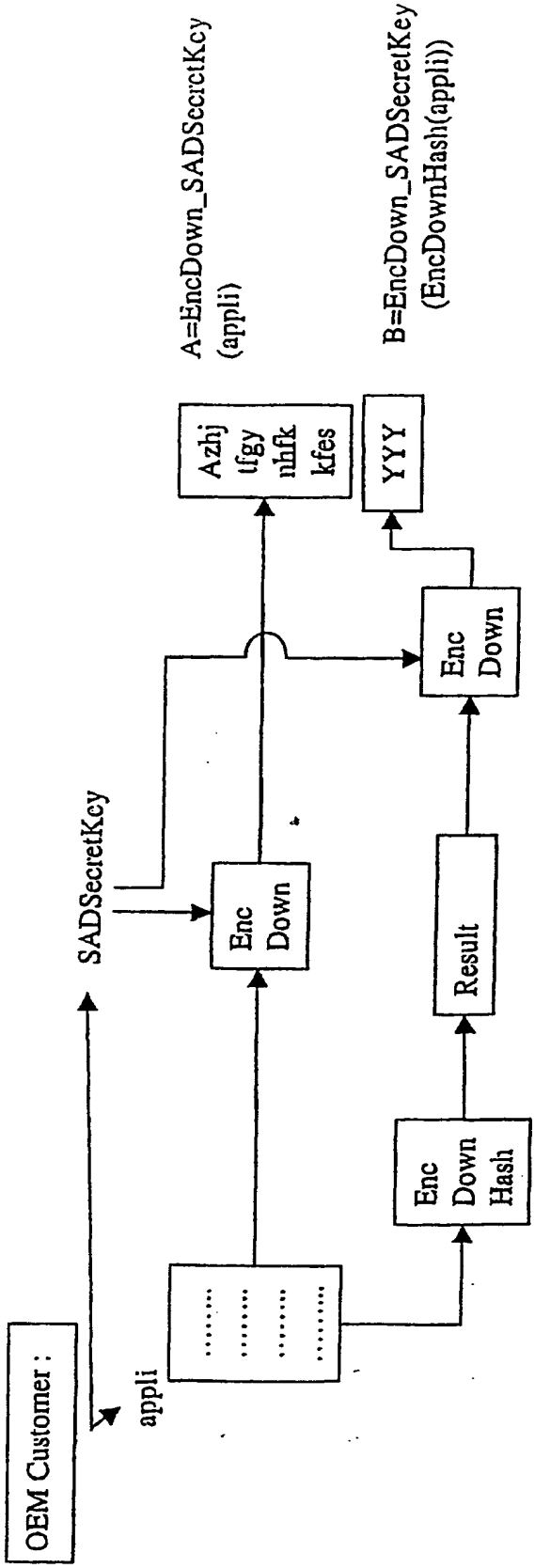


Figure 3D


C&D&E&F received by the ASIC
2nd option
{appli signed by CustomerPrivateKey}
(c)
{CustomerPublicKey with downloaded data}
SignDownHash(E)=E'
SignDownEnc-1_ SADPublicKey(F)=F'
No
Is E'=F'?
Erase C
Yes
CustomerPublicKey=E
SignDownEnc-1_CustomerPublicKey(D)=D'
SignDownHash(C)=C'
No
Is C'=D'?
Erase C
Yes
Validated Appli C
Store Appli in RAM using encryption hardware interface

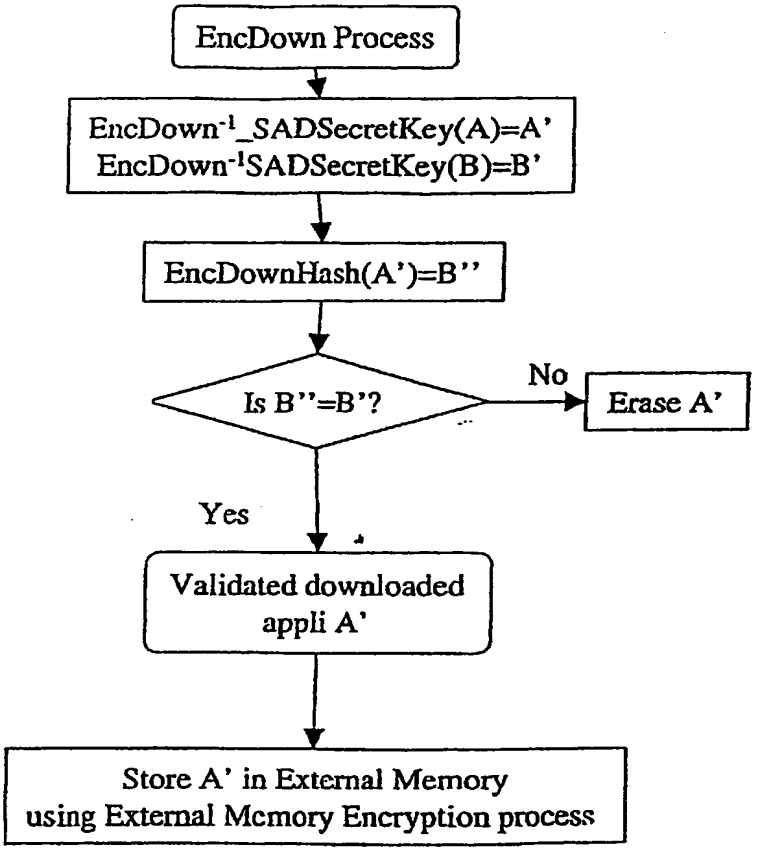
10/500983
Rec'd PCT/PTO 06 JUL 2004

Figure 4A



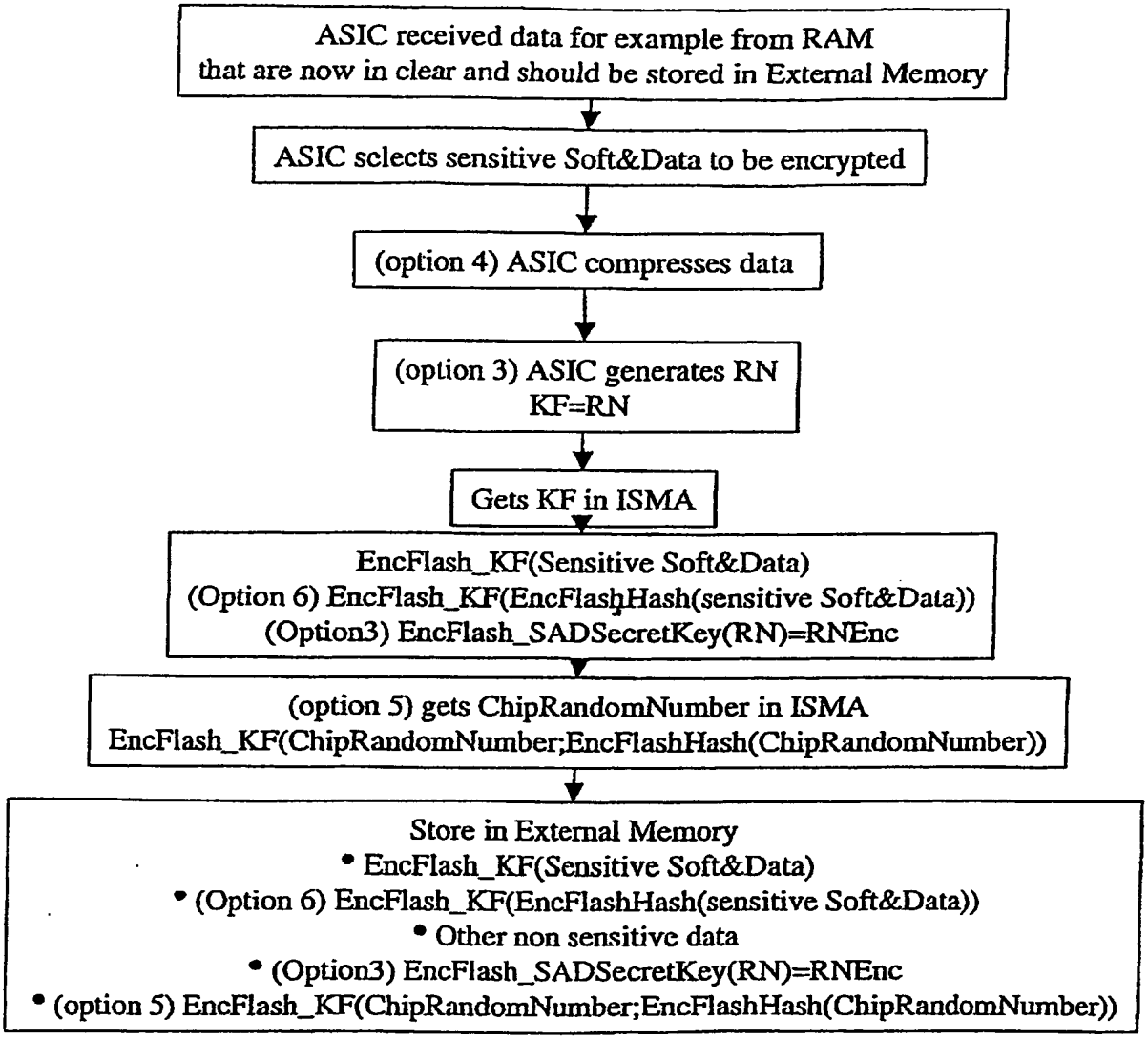
10/500983
Rec'd PCT/PTO 06 JUL 2004

Figure 4B



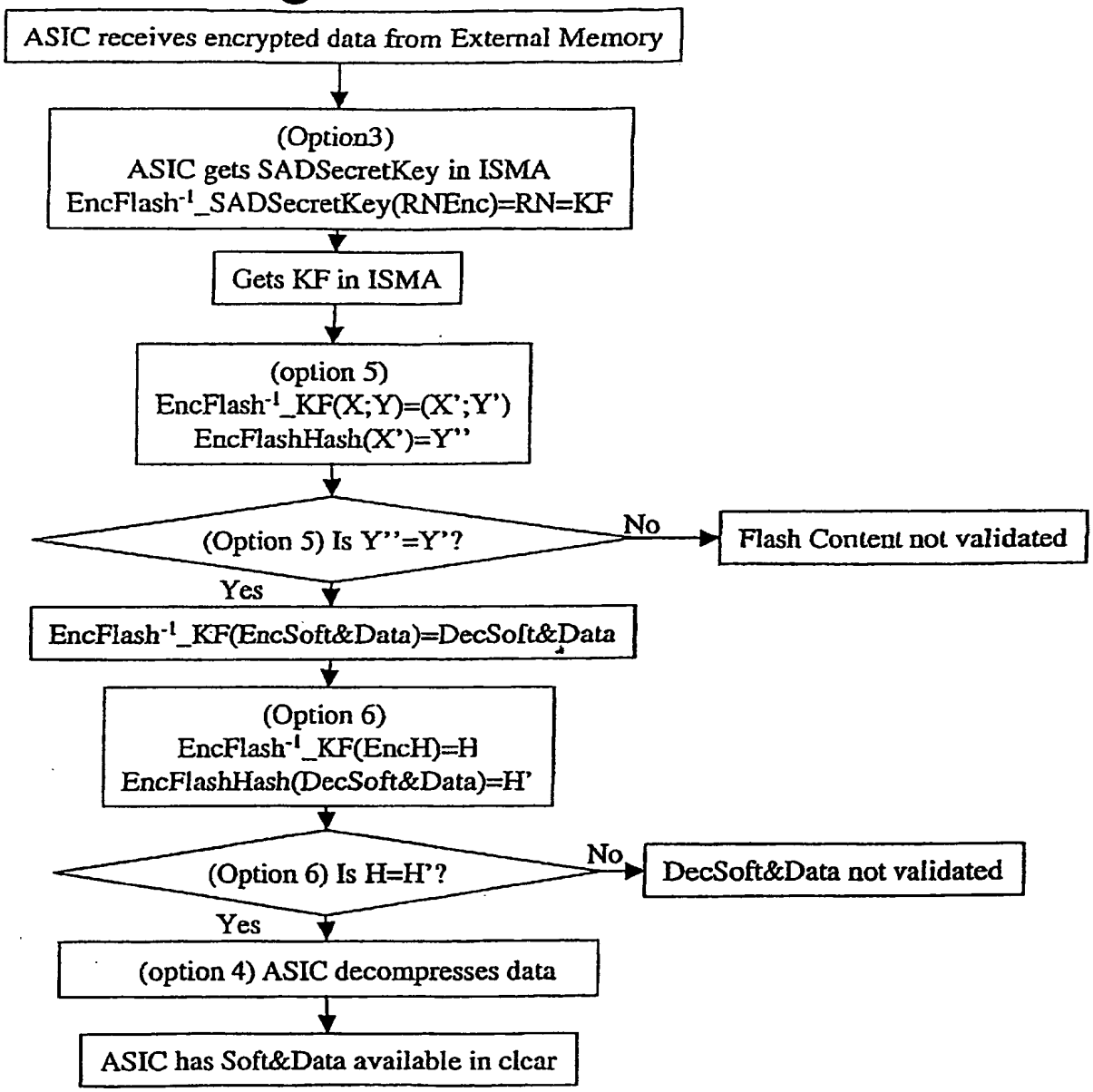
10/500983
Rec'd PCT/PTO 06 JUL 2004

figure 5A



10/500983
Rec'd PCT/PTO 06 JUL 2004

figure 5B



10/500983
Rec'd PCT/PTO 06 JUL 2004

figure 6

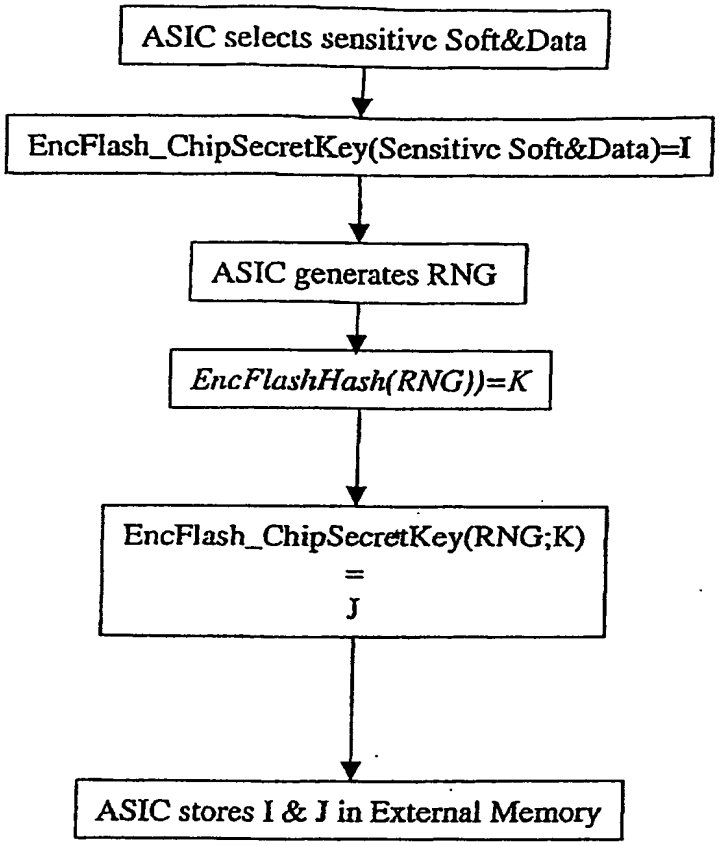
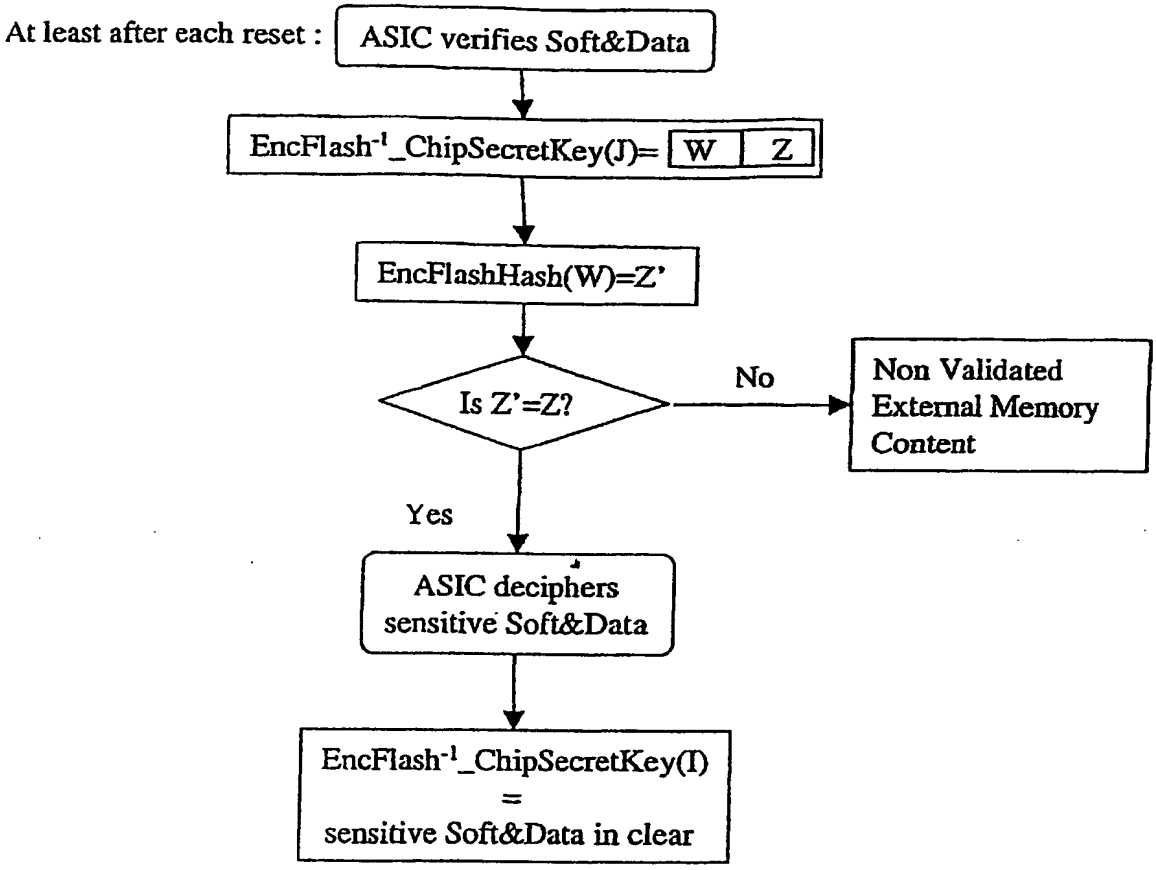
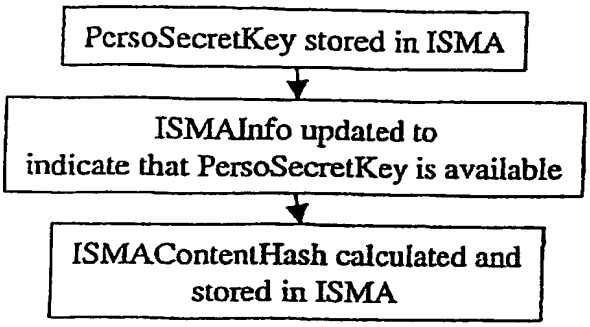


figure 7


At least after each reset :
ASIC verifies Soft&Data
EncFlash-1_ChipSecretKey(J)=
W
Z
EncFlashHash(W)=Z'
Is Z'=Z?
No
Non Validated External Memory Content
Yes
ASIC deciphers sensitive Soft&Data
EncFlash-1_ChipSecretKey(I) = sensitive Soft&Data in clear

10/500983
Rec'd PCT/PTO 06 JUL 2004

figure 8



ISMA after First level personalization

ASIC ISMA :

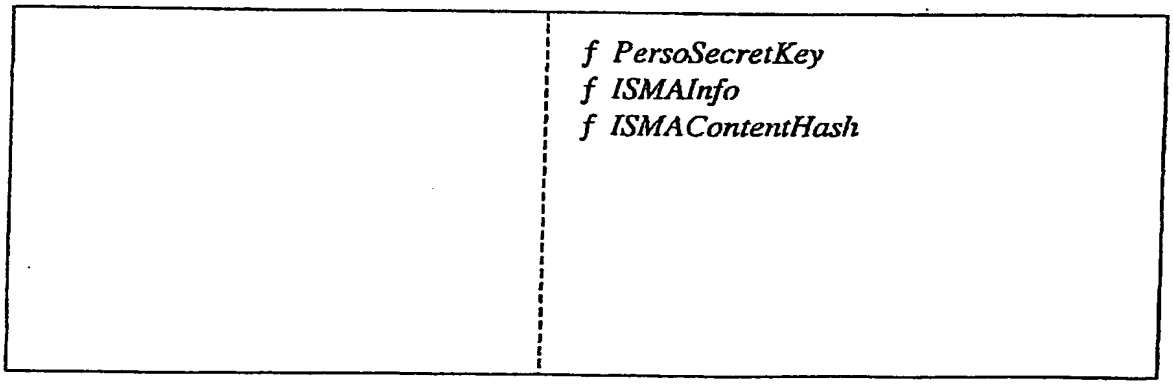


figure 9

- SignPersHash is a hash function used
- give a 20 Bytes result relevant to ersoAppli integrity
- SignPersEnc is an encryption ignature)algorithm used to encrypt the ash result asymmetrically with ADPrivateKey
- EncPers is an encryption symmetric ol used to encrypt the personalization ftware and eventually its signature

SAD provides personalization application PersoAppli to OEM customer

EncPers_PersoSecretKey(PersoAppli) & SignPersEnc_SADPrivateKey(SignPersHash(PersoAppli)) or EncPers_PersoSecretKey(PersoAppli;SignPersEnc_SADPrivateKey(SignPers Hash(PersoAppli)) downloaded by OEM customer

PersoAppli is available in a protected and signed format OEM Customer's ASIC having PersoSecretKey & SADPublicKey will be able to authenticate it, and then to unencrypt it.

ISMA after Second level personalization

ASIC ISMA :

	f Sensitive data *f ISMAInfo* *f ISMAContentHash*

PersoAppli will have the task
- to file ISMA with sensitive data
- erase PersoSecretKey
- update ISMAInfo
- Compute and write ISMAContentHash
- erase PersoAppli

PersoAppli will stored sensitive data corresponding to the different option corresponding to the OEM customer requirements. It could be run directly or stored in the External Memory using EncFlash_PersoSecretKey (means KF = PersoSecretKey).

Rec'd PCT/PTO 06 JUL 2004
10/500383

figure 10

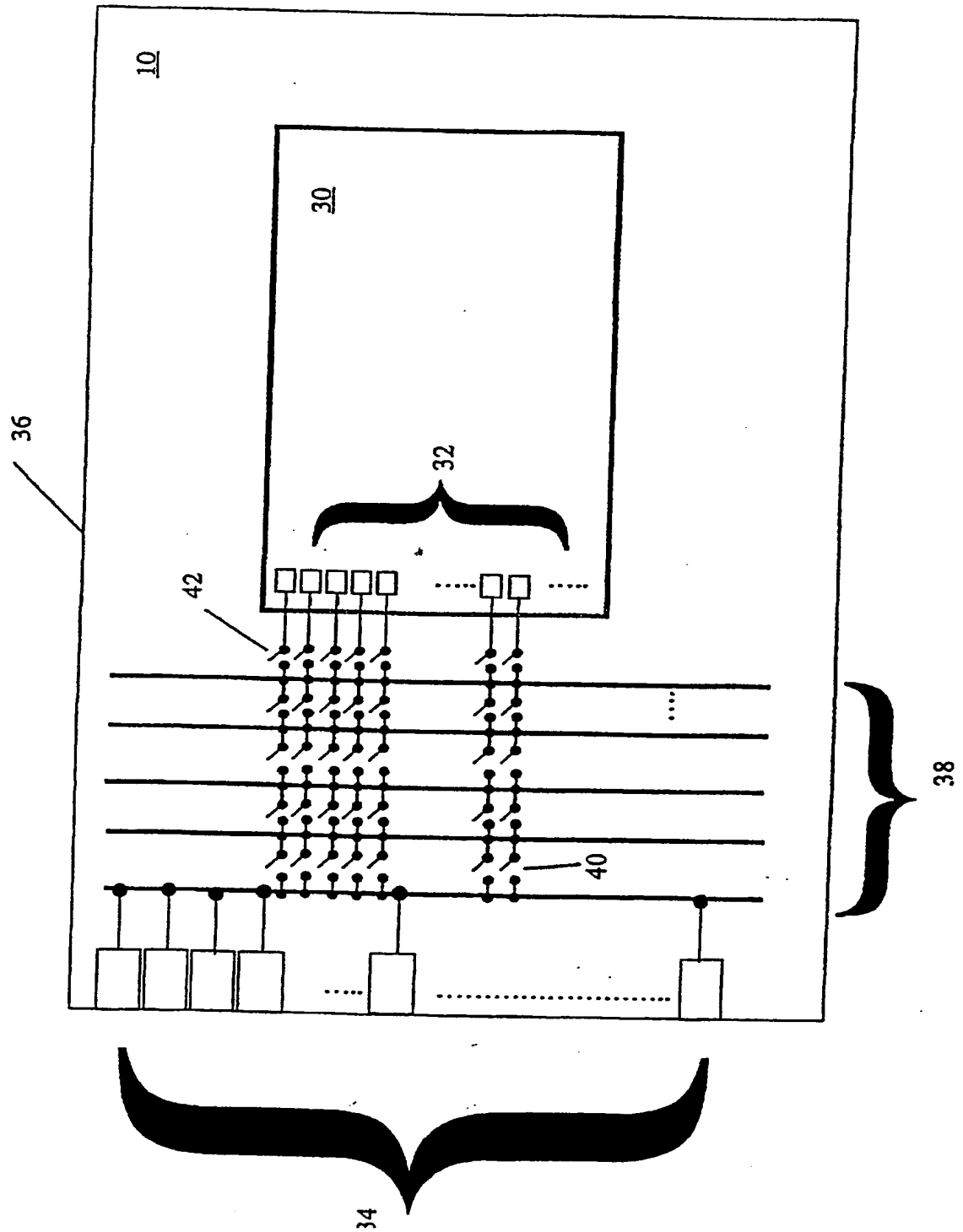
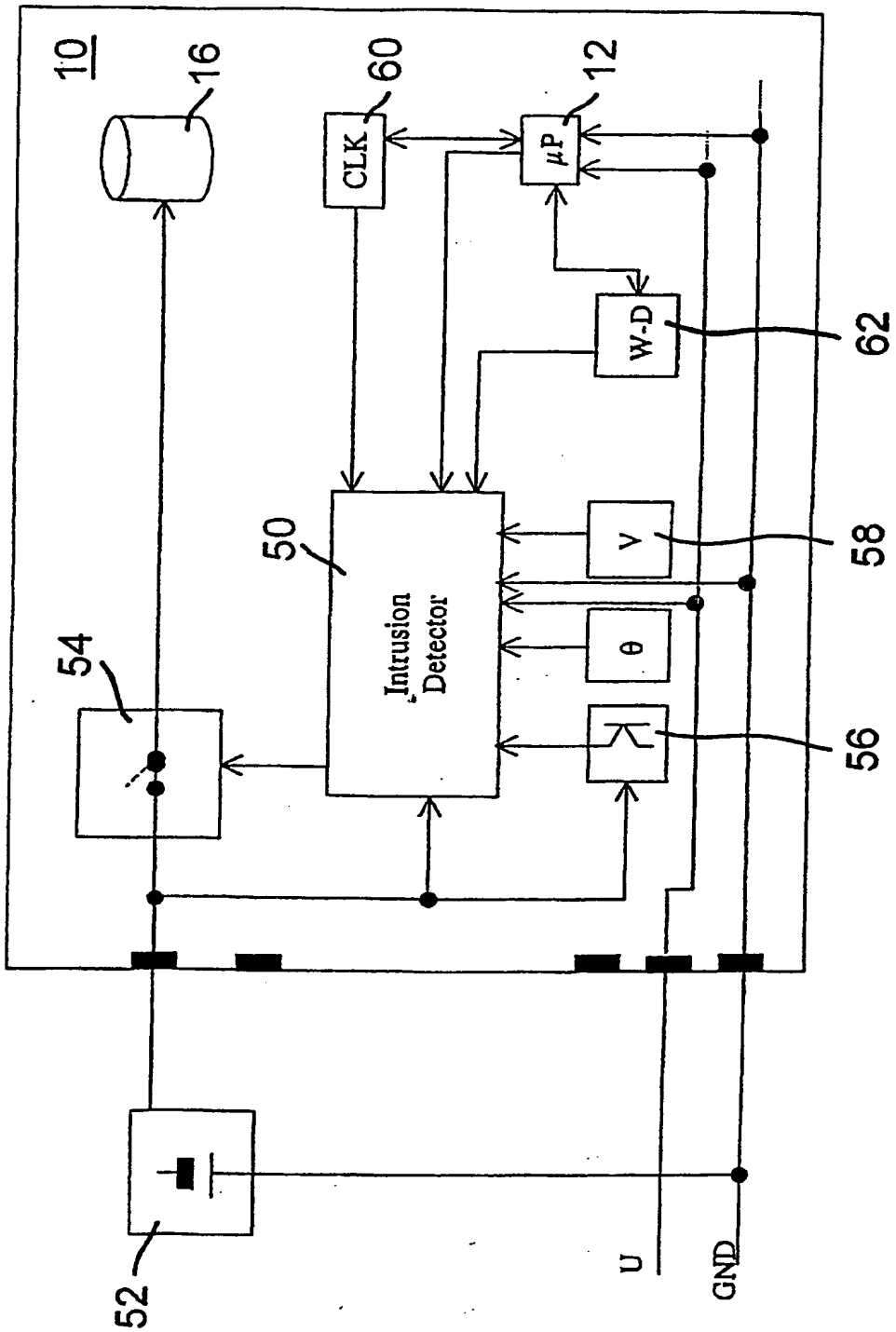


figure 11


10
16
60
12
CLK
µP
W-D
62
50
Intrusion Detector
V
58
θ
54
56
52
U
GND

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.